Imperva sonar and data security

The course design should include the following:

Imperva Sonar Foundations

- The capabilities and unique benefits of Imperva Sonar.
- The Sonar Architecture.
- Deployment Guidelines.
- Account Management.
- Data Set Queries.
- Working with Pipelines.
- Ticket Creation and Management.
- Identifying False Positives.
- Configure security monitoring with built-in models.
- Ingesting data from MSSQL, Oracle Unified and Maria DB.
- Ingesting Data from Azure and AWS platforms.
- Integrating Imperva On-Prem DAM and Splunk SIEM.

Data Security Fabric - Data Gateway

- How to initially configure SecureSphere for a Database Security deployment.
- How to run DB Data Classification Scans to find sensitive data.
- How to implement Database Security Policies and Database Auditing.
- How to configure DB Profiling.
- How to analyze Database Violations and Alerts.
- How to perform best practice tuning tasks.
- How to configure Active Blocking.
- How to configure Assessment Scans and manage risk scores.
- How to configure Database User Rights Management Scan and analyze the results.

Administering Imperva Security Infrastructure

- How to install and maintain SecureSphere system components including the Management Server, Gateway, and Agents.
- How to ensure connectivity among SecureSphere components and commonly integrated network devices.
- How to perform initial SecureSphere administration and configuration tasks that align with an organization's architecture and specific requirements or follow Imperva best practices.
- Common cross functional tasks such as object creation, policy creation, basic rule understanding, system alert interpretation, and report generation.

Data Risk Analytics (DRA)

- How to install the DRA Admin and Analytics Servers.
- How to integrate Active Directory into DRA Analytics.
- How to integrate DRA with several types of audit sources.
- How data flows through a DRA architecture.
- Confirm appropriate audit detail is received in DRA.
- Analyze Incidents to identify careless, compromised, or malicious activity.
- Analyze Incidents to identify false positive events.